In the Specification

Please replace paragraphs[0001] through [0003] with the following:

Related Application

This is a §371 of International Application No. PCT/FR03/00122, with an international filing date of January 15, 2003 (WO 03/063445, published July 31, 2003), which is based on French Patent Application No. 02/00635, filed January 18, 2002.

Field of the Invention

~~The present~~This invention pertains to the secure processing, broadcasting, recording and display of video data and television programs or more generally any multimedia program or sequence using a MPEG type nominal flow format, by authorized users and ~~proposes~~provides a secured system for the processing, broadcasting, delivery, recording, private copying and viewing of video or interactive multimedia programs and sequences.

Background

The general problem is to provide a device capable of transmitting in a secure manner a set of high visual quality films in an MPEG type format directly to a television screen and/or to be recorded on the hard disk of a box connecting the remote transmission network to the television screen, while preserving the audiovisual quality but preventing any fraudulent use such as the possibility of making pirate copies of films or audiovisual programs recorded on the hard disk of the decoder box.

~~The invention also enables complete control of the use of the copies and the rights of the broadcast works.~~

Please replace paragraph [0005] with the following:

However, the principal disadvantage of ~~all of the~~ presently available solutions ~~(TiVo Inc.,~~such as in WO 00/165762~~)~~ is that it is necessary to transmit not only the encrypted data to the users but also the decryption keys. Transmission of the decryption keys can be performed prior to, at the same time as or after transmission of the audiovisual programs. In order to increase the security and thus the protection of the audiovisual works against ill-intentioned use, the decryption keys as well as the decryption functions of the audiovisual decoders can comprise enhanced security means such as smart cards or other physical keys that can optionally be updated remotely.

Please replace paragraphs [0007] through [0014] with the following:

One solution would therefore consist of transmitting all or part of a digital audiovisual program solely on demand (on demand video services) via a broad-band telecommunication network of the DSL, cable or satellite type without authorizing the local recording of the audiovisual programs. The disadvantage ~~here~~there is completely different and stems from the performances of these network which do not make it possible to guarantee continuous flows of several megabits per second to each user as required by MPEG flows which require pass bands from several hundreds of kilobits to many megabits per second.

Under these conditions, one solution consists of separating the flow into two parts neither of which could be used by itself. Many patents have been filed in the context of this approach. We thus know from ~~document~~ WO 09/908428 ~~(Gilles Maton)~~ a method for the multiapplication processing of a localizable active terminal in which there is implemented at least one link with an identifiable program dedicated to the execution of an application, said program dictating its operating conditions to the terminal for the setting up of its functions. The terminal dialogues in a punctiform manner by using a link with the management center for the implementation, if necessary, of the

inputs and outputs of the capacities of this center with the management center optionally becoming the slave of the terminal at the application level in relation to the incoming program. ~~This~~That invention also pertains to the method for the identification of the program and the terminal in operating mode. ~~This~~That method of the prior art divides the flow into a part used for identifying the user and a part that contains the actual program itself. In particular, ~~said~~the program is not unusable but merely made inaccessible by the first part.

In addition, ~~document~~ EP 0778513 ~~(Matsushita)~~ describes a method enabling prevention of illegal use of an information unit by adding to it a control information unit in order to verify the rights of the user. The system makes it possible to remain permanently informed as to which part of the information unit is used and by which user and thereby to be informed as to whether or not this user is in an illegal position. ~~This~~That method thus makes the data secure by adding additional information units which distort the initial information.

~~Document~~ WO 00/49483 ~~(Netquartz)~~ also provides ~~us with~~ methods and systems for creating a link between the users and an editor of digitized entities. The method comprises at least one of the following steps: the step of subdividing said digitized entity into two parts; the step of storing one part in memory in a server connected to a computer-based network; the step of transmitting the other part to at least one user who has available computer-based equipment; the step of connecting said computer-based equipment to said computer-based network; the step of establishing a functional link between said first part and said second part. ~~These~~Those methods and systems do not specify whether the part stored in memory on the server can be stored by the user, which would enable the user to pirate said digitized entity.

Lastly, with regard to this approach, the closest state of the art is found in the patents of HyperLOCK Technologies, the most pertinent of which is ~~document~~ US 5,937,164. ~~This~~That

invention uses the solution comprised of separating the flow into two parts, the smaller one of which holds an information unit required for the use of the larger part. ~~This~~That patent nevertheless is not sufficient for resolving the identified problem. In fact, suppression of a part of the flow distorts the format of the flow which then cannot be recognized as a standard flow that can be run with general software applications. ~~This~~That method of the prior art requires both a specific software program at the server side for the separation of the two parts, and another specific software program enabling not only the reconstruction of the flow but also the acquisition of the principal flow and its management according to a format proprietary to the solution. ~~This~~That proprietary format is not the initial format of the flow prior to separation into two parts in this known solution.

~~This company has also filed three other patents: document~~ US 5,892,825 returns to the approach of the preceding patent but in a narrower framework because the flows are still encrypted; ~~document~~ US 6,035,329 is based on the same principle and pertains to a method enabling the reading of a CD-ROM or DVD-ROM disk contingent on the identification of the rights by the insertion of a smart card on which the information required for reading are stored. ~~This~~That method is still not adequate for our problem because it does not ensure that the modified flow is of the same format as the original flow. Finally, ~~document~~ US 6,185,306 pertains to a method for the transmission of encrypted data from a Web site to a requesting computer. ~~This~~That method, however, makes it possible for the user to have available at a given moment the tools required for copying the data.

Summary of the Invention

This invention relates to a method of distributing video sequences according to a nominal flow format including a succession of frames each including at least one I block corresponding to a complete digital I image and at least one N block corresponding to differences between a digital N image and at least one other image including analyzing the flow of sequences to generate a first

modified flow having a format of a nominal flow and having modified N blocks and a second flow of any format including digital information required to reconstruct the modified blocks; transmitting the first and second flows from a server to destination equipment, and calculating on the destination equipment a synthesis of a flow in a nominal format as a function of the first flow and the second flow.

This invention also relates to a system that creates a video flow according to the method, including at least one multimedia server containing original video sequences and a device for analyzing video flow originating from the server for generating the first and second flows.

This invention further relates to a system that manages a video flow according to the method, including a computer unit of a communication interface for receiving the video flow originating from a communication network or a physical support reader and equipped with at least one recorder that stores content of the first flow, a decoder including a display interface, means for communicating with the principal computer for receiving the first flow transmitted by the computer and communication means for receiving the second flow, and a means for recomposing original flow from the first and second flows.

This invention yet again relates to a system for transmitting a video flow according to the method, including an equipment unit that produces a video flow, at least one equipment unit that manages the video flow and at least one communication network between the production equipment and the management equipment unit(s).

Brief Description of the Drawings

Better understanding of the invention will be obtained from the description below of a nonlimitative example of implementation with reference to the attached drawings in which:

Fig. 1 describes the architecture of a system for the implementation of the method according to the invention; and

Fig. 2 represents one particular mode of implementation of the system for the analysis and synthesis of MPEG type flow in accordance with the invention.

Detailed Description

~~In order to correct these different shortcomings of the prior art, the~~This invention pertains in its broadest sense to a method for the distribution of video sequences according to a nominal flow format constituted by a succession of frames each comprising at least one I block corresponding to a complete digital I image and at least one N block corresponding to the differences between one digital image and at least one other image, characterized in that there is performed prior to the transmission to the client's equipment an analysis of the flow in order to generate a first modified flow presenting the format of a nominal flow and ~~presenting~~having modified N blocks and a second flow of any format comprising the digital information which can enable the reconstruction of ~~said~~the modified blocks, then of separately transmitting the two flows thereby generated from the server to the destination equipment, and in that there is calculated on the destination equipment a synthesis of a flow in the nominal format as a function of said first flow and said second flow.

~~Said~~The synthesis advantageously produces a flow rigorously identical to the original flow, i.e., the process is without loss.

Please replace paragraphs [0019] through [0023] with the following:

~~Said~~The analysis can advantageously determine the N images to be modified in order to obtain ~~said~~the first flow; these modifications can be: replace a P image by another P image from another flow, invert two P images of the same flow, invert a B image and a P image of the same flow.

In one particular implementation of this method, the transmission of ~~said~~the first flow is implemented via a material support distributed physically such as a CD-ROM, a DVD or a hard disk.

In another implementation of this method, the transmission of ~~said~~the first flow is implemented via a broad-band network (cable, satellite, optical fiber, airwaves) via a DSL (Digital Subscriber Line) type network, via a DAB network or via a local radio loop network (LRL).

According to the implementation of this method, the transmission of ~~said~~the second flow is implemented via a cable network, via a switched telephonic network (analog or digital), via a mobile telephonic network using the GSM, GPRS or UMTS standards, via an LRL network (local radio loop) or via a DSL network.

According to one particular variant of this method, transmission of ~~said~~the second flow is implemented via a broad-band network of the same type as the network used for ~~said~~the first flow, or via the same network.

Please replace paragraph [0028] with the following:

The invention moreover pertains to an equipment unit for the creation of a video flow for the implementation of this method comprising at least one multimedia server containing the original video sequences and characterized in that it comprises a device for the analysis of the video flow stemming from ~~said~~the server in order to generate the two flows.

Please replace paragraphs [0030] through [0035] with the following:

The invention moreover pertains to equipment for the management of a video flow for the purpose of implementing this method comprising a standard flow decoder, at least one recording interface (hard disk, flash memory, etc.) intended to store the contents of ~~said~~the first flow and/or a disk reader (CD, DVD, etc.) and at least one display interface (standard screen, wireless screen,

video projector), characterized in that it comprises a means for the recomposition of the original flow from the two flows.

According to one particular mode of implementation, ~~said~~the means is a software application installed in the equipment.

According to another mode of implementation, ~~said~~the means is a fixed electronic device.

According to another mode of implementation, ~~said~~the means is a portable or mobile electronic device.

According to a mode of implementation in which the equipment is installed on a computer, ~~said~~the means uses a resource specific to the product (card) so as to prevent the copying of the temporary information of the second flow onto a permanent support.

~~Said~~The recording interface advantageously also stores a "private copy" marker in relation to ~~said~~the first flow indicating for this sequence the rights of the user: private copy that can be viewed an unlimited number of times, private copy that can be watched a limited number of times and specification of that number, private copying prohibited.

Please replace paragraphs [0039] through [0040] with the following:

According to a first mode of implementation, ~~said~~the means for the recomposition of the flow is a software application installed solely on ~~said~~the decoder.

According to a second mode of implementation, ~~said~~the means for the recomposition of the flow is an electronic device installed solely on ~~said~~the decoder.

Please delete paragraph [0042].

Please replace paragraph [0045] with the following:

The general principle of a method to ensure the security of a video flow is presented below. The objective is to authorize on demand video and upon demand via all of these broadcasting

networks and the local recording in the user's digital decoder box. The solution consists of permanently preserving outside of the user's habitation, in fact in the broadcasting and transmission network, a part of the recorded audiovisual program, this part being essential for viewing ~~said~~the audiovisual program on a television or monitor screen, but being of very small volume in relation to the total volume of the digital audiovisual program recorded by the user. The missing part will be transmitted via the broadcasting and transmission network at the time of viewing said digital audiovisual program prerecorded by the user.

Please replace paragraphs [0047] through [0049] with the following:

Fig~~ure~~. 1 in the attached drawings is a diagram of the principle of a distribution system according to the present invention.

Fig~~ure~~. 2 represents a particular mode of implementation of the system for the analysis and synthesis of MPEG flow according to the invention.

In ~~figure~~Fig. 1, the video interface (8) setup is adapted for connecting at least one display device, e.g., a monitor, a video projector or a television screen type device (6) to at least one broad-band transmission and broadcasting network (4) interface and to at least one telecommunication network interface (10). According to the ~~present~~ invention, this setup is composed of a module (8) comprising principally a suitable processing unit for processing, in particular decoding and unscrambling, all MPEG type video flows according to a preloaded decoding and unscrambling software program in real or delayed time, of storing it, recording it and/or transmitting it on a telecommunications network, as well as a screen interface (7) and an interface for connection to a local or extended area network (5) and/or (9). The broad-band transmission and broadcasting network (4) and the telecommunication network (10) can be a single network.

Please replace paragraph [0051] with the following:

As shown in ~~figure~~Fig. 1, the connection interface (5) is linked to a broad-band transmission and broadcasting network (4) such as a modem, a satellite modem, a cable modem, an optical fiber line or a radio or infrared interface for wireless communication.

Please replace paragraph [0057] with the following:

Three major types of images are thus defined in order to respond to the contradictory demands of a possibility of direct access and a high compression efficacy.

1. The Intra coding images (I images) are coded without reference to the other images. They provide the access points to the coded sequence in which the decoding can commence but are coded with a moderate compression rate.

2. The Prediction coded images (P images) ~~present~~have a more effective coding using a movement-compensated prediction after a prior intra (I) or predicted (P) image, and are generally used as reference for a future prediction.

3. The images coded by Bidirectional prediction (B images) provide the highest compression rate, but require for movement compensation a prior reference image and a future reference image. The images coded by bidirectional prediction are never used as prediction reference.

Please replace paragraphs [0064] through [0065] with the following:

As shown in ~~figure~~Fig. 1, the connection interface (9) is linked to an extended telecommunication network (10) directly or via a local network serving as access network and it is constituted, e.g., by a subscriber line interface (analog or digital telephonic network, DSL, LRL, GSM, GPRS, UMTS, etc.).

Thus, the audiovisual programs are broadcast in a conventional manner in multidiffusion mode ("broadcast") via the broad band transmission network (4) of the airwaves, cable, satellite, digital airwaves, DAB, DSL type, etc., from the server (1) directly via the link (3 bis) or via the portal (12) via the link (2) and (3) to the decoder module (8) by means of the link (5). Each audiovisual program broadcast in this manner can be optionally encrypted and in accordance with the ~~present~~ invention, the MPEG flow contains modifications at the level of the B and/or P images as described above. As a function of the parameters selected by the user or of the information transmitted by the broadcast server, certain audiovisual programs modified in this manner and incomplete are recorded on the hard disk of the box (8).

Please replace paragraphs [0069] through [0075] with the following:

According to a particular mode of implementation, the box (8) comprises a smart card reader which enables the portal (12) to authenticate the user owner of the box (8). If this is authorized, this function also allows the user to make private copies of the audiovisual programs recorded on the hard disk of his decoder box (8). In order to do this, if the user wants to make a private copy of an audiovisual program, ~~he~~the user does so in the conventional manner on a VCR via the link (7) that connects the box (8) to the display screen (6).

However, if the user wants to preserve a private copy on the hard disk of ~~his~~the box, ~~he~~the user will so inform the box (8) which will record the "private copy" information unit as well as the coordinates of the user which are on the smart card in a particular field (84) of this audiovisual program recorded on the hard drive (85) of the decoder box (8). Whenever the user subsequently wants to watch this private copy, the box (8) will connect automatically to the portal (12) and inform the box that the user wants to implement a reading of his private copy; in response, if the reading of the private copy is possible for this user who possesses this smart card linked to this box (8), the

decoder box (8) will then receive the missing B and/or P images as well as all the other information enabling the display of the audiovisual program constituting the private copy.

According to another mode of implementation, if the user wants to preserve a private copy on the hard drive of ~~his~~the box, ~~he~~the user will so inform the server which will record the information unit "private copy" for this program and for this user authenticated by the smart card. Each time that the user wants to watch this private copy, the box (8) will then connect automatically to the portal (12) and will inform this portal that the user wants to implement a reading of ~~his~~the user's private copy; in response, if the reading of the private copy is possible for this user who possesses this smart card and for this program, the decoder box (8) will then receive the missing B and/or P images as well as all of the other information enabling the viewing of the audiovisual program constituting the private copy.

According to a particular mode of implementation, the so-called "private copy" could enable the user to watch this same audiovisual program in an unlimited manner or a number of times determined in advance by the service provider who authorized this private copy.

The ~~present~~ invention also pertains to the physical box (8) used by the consumer to access the data. This physical box is located at the user's domicile. It provides a set of functionalities which manage the appropriate information to be presented according to the audience's selection and manages the connection and communication with the remote server.

According to a particular mode of implementation, the physical box (8) corresponding to the video interface setup ~~(8)~~ is implemented as a fixed autonomous device with integrated hard disk.

According to another particular implementation, the video interface setup ~~(8)~~ is implemented as an add-on card which would be installed in a PC-type computer and would be linked to at least one broad-band transmission and broadcasting network interface (4) and to at least one

telecommunication network interface (10). This card would use the hard disk of the PC for recording the first flow, but would have its own calculator and its own volatile memory so as to not allow the ill-intentioned user of the PC the means to access the complementary information units such as the B and/or P images of the second flow.

Please replace paragraphs [0077] through [0081] with the following:

It lastly should be noted that the invention degrades the MPEG flow from the visual point of view until no longer allowing recognition of the transmitted and displayed scenes without having access to the complementary data and characteristics, but completely reconstitutes the MPEG flow in the video interface setup ~~(8)~~ without any loss.

Although the ~~present~~ invention has focused most particularly on audiovisual data, it is understood that all interactive multimedia information and all interactive data can be processed by the ~~present~~ setup and the ~~present~~ system, MPEG type video data being the most elaborated. Better understanding of the ~~present~~ invention will be obtained from the description below ~~presenting~~describing the physical basis of the ~~present~~ invention and with reference to ~~figure~~Fig. 2 of the attached drawings representing a preferred mode of implementation of this latter setup as a nonlimitative example of implementation particularly suitable for cable and satellite networks. The complete MPEG flow (101) is analyzed by the analysis device (121) of the portal (12) and will thus be separated into an MPEG type flow but whose B and/or P images will have been processed and sent via the output (122) of the portal to the broad band transmission and broadcasting network (4).

The other part of the modified MPEG flow will be stored in memory in the buffer memory (122) of the portal (12). For each MPEG flow broadcast in this manner, the portal (12) will store in a buffer memory (122) the modifications that were implemented in this MPEG flow by the analyzer (121) of the portal (12). It should be clarified that for the same incoming MPEG flow (101)

the processing of the flow can be different for each user (18) and/or for each group of users (18). Thus, the buffer (123) of the portal (12) comprises a different memory zone for each user.

In the implemented examples, for a first user (18) each first P image of the MPEG flow which follows an I image was replaced by a random P image of the same type and same volume as the P image removed in this manner. It has been found that the degrading effects on the output flow are very intense.

For a second user (18) the nth P image that follows each I image of the MPEG flow was permuted by and with the first B image that follows this P image. It has been found that this permutation is very effective for MPEG type animated sequences compared to MPEG sequences ~~presenting~~having little animation.

Please replace paragraphs [0083] through [0090] with the following:

The portal (121) selected the MPEG flow (101) that it must transmit to the user (18) to be watched on a delayed basis on his television screen (6). This user is linked to a digital cable broadcast network (4) offering video on demand (VOD), the network (10) is thus the same as the network (4). The analysis system (121) of the portal (12) will thus read the incoming MPEG flow (101) and each time that it detects an I image, it searches for the first P image that follows this I image so as to replace it with a random P image that it calculated. The new modified MPEG flow is then recorded in the output buffer (122) to be broadcast on the broadcast network (4) via the link (5). The P images removed from the incoming MPEG flow (101) are stored in the buffer memory (123) of the portal. In the implemented example, rather than substitute each P image that follows an I image, the analysis system (12) only takes one I image out of n in which n is a random number comprised between 1 and 7. When the analysis system (121) writes the substituted P image in the

buffer memory (123), it also writes the number of the I image that precedes the thereby substituted P image. The analysis system (121) continues its analysis until the end of the incoming MPEG flow.

During this time and in a completely unsynchronized manner, the outgoing modified MPEG flow originating from the output buffer (122) of the portal (12) is broadcast via the broad band network (4) to one or more users (18).

Each decoder box (8) from Fig. 1 (that is essentially a user 18 in Fig. 2) that wants to record this MPEG flow modified in this manner can then read this MPEG flow and record it on its hard disk (85). This recording initiative is left to the decoder box (8) under the control of the portal (12). In order to perform this, the analysis system (121) had written at the beginning of the MPEG flow an information unit of supplementary data that specified the addresses of this modified MPEG flow. The addressees can thus be a particular and single addressee/user (18), a group of addressees/users (18) or the totality of the decoder[[s]] boxes (8) from Fig. 1 linked to the network (4).

The phase described above corresponds to the first phase of preparation of the MPEG flow by the portal (12), its transmission via the broad band network (4) and its recording in a decoder box (8) from Fig. 1. This decoder can then display this MPEG flow recorded on its hard disk (85). In order to perform this, the synthesis system (87) of the decoder box (8) in Fig. 1/user (18) will read the MPEG file from its hard disk (85) and will send it to a conventional MPEG reader (81). If no complementary data is received by the synthesis system (87), then the MPEG flow which reaches the reader (81) is processed and displayed as it is, which causes a huge distortion of the display on the display screen (6). In effect, the substituted P images which are processed by the synthesis system (87) do not correspond to the P images which are required for a correct viewing because certain P images were replaced by random P images. In contrast, since the recorded flow is definitely an MPEG type flow, the reader (81) does not discriminate and displays the information

on the output screen (6) where it gives the appearance of an MPEG video flow but which is totally incoherent for the human being who watches the screen (6). Any copy of the MPEG flow originating from the hard disk (85) of the box (8)/user (18) would produce the same visual effect when it is reconstituted by any MPEG reader; all uses of this copy which would be ill-intentioned are thus doomed to failure.

When the user ~~of the decoder~~ (18) wants to correctly display on his screen (6) the audiovisual program recorded on his hard disk (85), ~~he~~the user sends ~~his~~a request to the synthesis system (87) with ~~his~~a remote controller as ~~he would~~ with a VCR or DVD reader presenting a menu on ~~his~~a television screen. The synthesis system (87) then issues a request to the hard disk (85) and commences to analyze the modified MPEG flow originating from the hard disk (85) via the reading buffer (83). The synthesis system (87) then establishes a link with the portal (12) via the telecommunication network (10) which in ~~our~~the example is also the cable network, but which can be a conventional telephone network or a DSL link. Once this link has been established, and during the entire duration of watching the film or audiovisual program, the synthesis system (87) draws out from the buffer memory (123) of the server (12) the substituted P images and the data corresponding to the positions of these P images in relation to the I images of the flow recorded on the hard disk. These P images and these position data are drawn out from the synthesis system (87) via the input buffer memory (86) and are stored temporarily in the volatile memory (88) of the synthesis system (87). From the modified MPEG flow that is drawn out via the buffer (83) and from the P images and the associated data that are drawn out via the buffer (86) in the memory (88), the synthesis system reconstitutes, in reverse manner of the previously described analysis process, the P images substituted by the real P images and sends the thereby reconstituted new MPEG flow to the reader

(81) to be displayed correctly on the screen (6). Upon their use, the P images to be substituted and the data associated with these P images are erased from the volatile memory (88).

In the implemented example, before the portal (12) authorized the transmission of the P images and the associated data from its buffer (123), the portal (12) had verified that the user ~~of the box~~ (18) was in fact authorized to receive them. In order to implement this step, the portal (12) reads the information contained on the smart card (82) of the user (18)/box (8) and verifies that the user is in fact authorized to watch this audiovisual program. It is not until this verification has been performed that the P images and the associated data are sent from the buffer (123) to the box user (18)/(8) corresponding to this user.

In the implemented example, the user had made a private copy of his audiovisual program. The synthesis system (87) therefore wrote complementary data on a part (84) of the hard disk (85) as well as the number of the smart card (82) and the information unit "private copy" as data associated with this audiovisual program. Upon the next private reading of this audiovisual program, the synthesis system (87) will analyze these associated data and then inform the portal (12) that the user ~~of the decoder~~ (18) is implementing a reading of the private copy. If this function is authorized for this user (18) by the portal (12), the P images and the associated data will then be sent by the portal (12) to the buffer (86) as described above. In the contrary case, the data will not be sent and the user ~~of the decoder~~ (18) will not be able to watch the reconstituted MPEF flow.

We will now describe in detail the different steps for the second user (18).

Please replace paragraphs [0092] through [0093] with the following:

In a manner identical to the description above, the user ~~of the decoder~~ (18) will receive the MPEG flows and the complementary data from the portal (12). In contrast, before sending the MPEG flow from the output buffer (122), the analysis system (121) will read the incoming MPEG

flow (101) and drawing a random number n comprised between 1 and 4, the synthesis system permutes the nth image P which follows each I image of the MPEG flow with the first B image that follows this P image. Each random number used in this manner is recorded in the buffer memory (123) of the portal (12).

During the reconstitution of the MPEG flow by the synthesis system (87) of the decoder box (8), the reading of these random numbers from the portal (12) and the reading of the MPEG flow modified in this manner from the hard disk (85) of the box (8) enables the synthesis system (87) to restore the B and P images in the correct order and send all of it to the reader (81).